WHAT IS CLAIMED IS:

1. A computer system comprising:

at least one processor;

a memory;

a secure platform stored in the memory for controlling the processor and the memory;

an operating system image stored in the memory for controlling the processor and the memory and operating on top of the secure platform;

an end user application stored in the memory for controlling the processor and the memory and operating on top of the operating system image; and

wherein the secure platform is configured to provide a secure partition within the memory for storing secret data associated with and accessible by the end user application, the secure partition being inaccessible to the operating system and other tasks operating on top of the secure platform.

2. The computer system of claim 1, wherein the at least one processor has at least three execution privilege levels including a first privilege level, a second privilege level that is less privileged than the first privilege level, and a third privilege level that is less privileged than the second privilege level.

3. The computer system of claim 2, wherein the end user application is configured to operate at the third privilege level as an unprivileged task, the operating system image is configured to operate at the second privilege level as an unprivileged task, and at least a first portion of the secure platform is configured to operate at the first privilege level as a privileged task.

4. The computer system of claim 3, wherein the first portion of the secure platform is a secure platform kernel (SPK).

5. The computer system of claim 4, wherein the SPK performs security critical services including memory services.

6. The computer system of claim 5, wherein the security critical services performed by the SPK further include process services, cryptographic services, and exception handling.

7. The computer system of claim 1, wherein the at least one processor includes:

protection key registers configured to hold protection keys, which the secure platform employs to control access to security critical structures.

8. The computer system of claim 7, wherein the security critical structures include the secure partition.

9. The computer system of claim 8, wherein the secure partition includes at least one memory page.

10. The computer system of claim 7, wherein the security critical structures include the end user application.

11. The computer system of claim 1, wherein the end user application includes a secure process indicator for indicating that the end user application is to be treated as a secure process.

12. A method of controlling a computer system, the computer system including a memory and at least one processor having at least three execution privilege levels, the execution privilege levels including a first privilege level, a second privilege level that is less privileged than the first privilege level, and a third privilege level that is less privileged than the second privilege level, the at least one processor also having protection key registers configured to hold

protection keys that are employed to control access to security critical structures, the method comprising:

operating a secure platform kernel (SPK) at the first privilege level as a privileged task;

operating an operating system at the second privilege level as an unprivileged task;

operating an end user application at the third privilege level as an unprivileged task;

allocating a portion of the memory for use by the end user application;

associating a first protection key value with the allocated memory portion;

inserting the first protection key value in one of the protection key registers only when instructions of the end user application are being executed, thereby allowing the end user application to access the allocated memory portion and preventing other tasks operating at the second and the third privilege levels from accessing the allocated memory portion.

13. The method of claim 12, and further comprising:

monitoring execution of instructions of the end user application; and

flushing the first protection key value from the protection key registers when execution of the end user application instructions stops.

14. The method of claim 13, and further comprising:

reinserting the first protection key value in one of the protection key registers when execution of the end user application instructions resumes.

15. The method of claim 12, wherein the allocating a portion of the memory is performed by the SPK.

16. The method of claim 12, wherein the first protection key value is inserted in one of the protection key registers by the SPK.

17. The method of claim 12, and further comprising:

associating a second protection key with the end user application to prevent unauthorized modification.

18. A computer system comprising:

at least one processor having at least three execution privilege levels, the execution privilege levels including a first privilege level, a second privilege level that is less privileged than the first privilege level, and a third privilege level that is less privileged than the second privilege level;

a memory;

an end user application stored in the memory for controlling the processor and the memory, the end user application configured to operate at the third privilege level as an unprivileged task;

an operating system stored in the memory for controlling the processor and the memory, the operating system configured to operate at the second privilege level as an unprivileged task;

a secure platform stored in the memory for controlling the processor and the memory, at least a first portion of the secure platform configured to operate at the first privilege level as a privileged task, the secure platform configured to provide a secure storage area in the memory for data associated with the end user application, the secure storage area accessible to a properly authenticated user of the end user application, the secure storage area inaccessible to other tasks operating at the second and third privilege levels, including the operating system.

19. The computer system of claim 18, wherein the first portion of the secure platform is a secure platform kernel (SPK).

20. The computer system of claim 19, wherein the SPK performs security critical services including memory services.

21. The computer system of claim 20, wherein the security critical services performed by the SPK further include process services, cryptographic services, and exception handling.

22. The computer system of claim 18, wherein the at least one processor includes:

protection key registers configured to hold protection keys, which the secure platform employs to control access to security critical structures.

23. The computer system of claim 22, wherein the security critical structures include the secure storage area.

24. The computer system of claim 23, wherein the secure storage area includes at least one memory page.

25. The computer system of claim 22, wherein the security critical structures include the end user application.

26. A computer readable medium containing a secure platform, an operating system image, and an end user application configured for controlling a computer system to perform a method, the computer system having a memory and at least one processor, the method comprising:

controlling the processor and the memory with the secure platform;

controlling the processor and the memory with the operating system image which operates on top of the secure platform;

controlling the processor and the memory with the end user application which operates on top of the operating system image; and

creating a secure partition within the memory for storing secret data associated with and accessible by the end user application, the secure partition being inaccessible to the operating system image and other tasks operating on top of the secure platform.